

ASSEMBLY BILL

No. 2828

Introduced by Assembly Member Chau

February 19, 2016

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

AB 2828, as introduced, Chau. Personal information: privacy: breach.

Existing law requires a person or business conducting business in California and any agency, as defined, that owns or licenses computerized data that includes personal information, as defined, to disclose a breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person in the most expedient time possible and without unreasonable delay, as specified.

This bill would also require a person or business conducting business in California, and any agency, that owns or licenses computerized data that includes personal information to disclose a breach of the security of the data to a resident of California whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person if the encryption key or security credential, as defined, has, or is reasonably believed to have been, acquired by an unauthorized person at any time before or after the breach of security of the data.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized ~~person~~ *person, or, if the encryption key or security credential has, or is reasonably believed to have been, acquired by an unauthorized person at any time before or after the breach of security of the data, to a resident of California whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.* The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More

Information.” Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22	<div>What You Can Do.</div> <div>Other Important Information. [insert other important information]</div> <div>For More Information.</div>	<div></div> <div>Call [telephone number] or go to [Internet Web site]</div>
---	---	---

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

1 (D) Whether the notification was delayed as a result of a law
2 enforcement investigation, if that information is possible to
3 determine at the time the notice is provided.

4 (E) A general description of the breach incident, if that
5 information is possible to determine at the time the notice is
6 provided.

7 (F) The toll-free telephone numbers and addresses of the major
8 credit reporting agencies, if the breach exposed a social security
9 number or a driver's license or California identification card
10 number.

11 (3) At the discretion of the agency, the security breach
12 notification may also include any of the following:

13 (A) Information about what the agency has done to protect
14 individuals whose information has been breached.

15 (B) Advice on steps that the person whose information has been
16 breached may take to protect himself or herself.

17 (e) Any agency that is required to issue a security breach
18 notification pursuant to this section to more than 500 California
19 residents as a result of a single breach of the security system shall
20 electronically submit a single sample copy of that security breach
21 notification, excluding any personally identifiable information, to
22 the Attorney General. A single sample copy of a security breach
23 notification shall not be deemed to be within subdivision (f) of
24 Section 6254 of the Government Code.

25 (f) For purposes of this section, "breach of the security of the
26 system" means unauthorized acquisition of computerized data that
27 compromises the security, confidentiality, or integrity of personal
28 information maintained by the agency. Good faith acquisition of
29 personal information by an employee or agent of the agency for
30 the purposes of the agency is not a breach of the security of the
31 system, provided that the personal information is not used or
32 subject to further unauthorized disclosure.

33 (g) For purposes of this section, "personal information" means
34 either of the following:

35 (1) An individual's first name or first initial and last name in
36 combination with any one or more of the following data elements,
37 when either the name or the data elements are not encrypted:

38 (A) Social security number.

39 (B) Driver's license number or California identification card
40 number.

1 (C) Account number, credit or debit card number, in
2 combination with any required security code, access code, or
3 password that would permit access to an individual's financial
4 account.

5 (D) Medical information.

6 (E) Health insurance information.

7 (F) Information or data collected through the use or operation
8 of an automated license plate recognition system, as defined in
9 Section 1798.90.5.

10 (2) A user name or email address, in combination with a
11 password or security question and answer that would permit access
12 to an online account.

13 (h) (1) For purposes of this section, "personal information"
14 does not include publicly available information that is lawfully
15 made available to the general public from federal, state, or local
16 government records.

17 (2) For purposes of this section, "medical information" means
18 any information regarding an individual's medical history, mental
19 or physical condition, or medical treatment or diagnosis by a health
20 care professional.

21 (3) For purposes of this section, "health insurance information"
22 means an individual's health insurance policy number or subscriber
23 identification number, any unique identifier used by a health insurer
24 to identify the individual, or any information in an individual's
25 application and claims history, including any appeals records.

26 (4) For purposes of this section, "encrypted" means rendered
27 unusable, unreadable, or indecipherable to an unauthorized person
28 through a security technology or methodology generally accepted
29 in the field of information security.

30 (i) For purposes of this section, "notice" may be provided by
31 one of the following methods:

32 (1) Written notice.

33 (2) Electronic notice, if the notice provided is consistent with
34 the provisions regarding electronic records and signatures set forth
35 in Section 7001 of Title 15 of the United States Code.

36 (3) Substitute notice, if the agency demonstrates that the cost
37 of providing notice would exceed two hundred fifty thousand
38 dollars (\$250,000), or that the affected class of subject persons to
39 be notified exceeds 500,000, or the agency does not have sufficient

1 contact information. Substitute notice shall consist of all of the
2 following:

3 (A) Email notice when the agency has an email address for the
4 subject persons.

5 (B) Conspicuous posting, for a minimum of 30 days, of the
6 notice on the agency's Internet Web site page, if the agency
7 maintains one. For purposes of this subparagraph, conspicuous
8 posting on the agency's Internet Web site means providing a link
9 to the notice on the home page or first significant page after
10 entering the Internet Web site that is in larger type than the
11 surrounding text, or in contrasting type, font, or color to the
12 surrounding text of the same size, or set off from the surrounding
13 text of the same size by symbols or other marks that call attention
14 to the link.

15 (C) Notification to major statewide media and the Office of
16 Information Security within the Department of Technology.

17 (4) In the case of a breach of the security of the system involving
18 personal information defined in paragraph (2) of subdivision (g)
19 for an online account, and no other personal information defined
20 in paragraph (1) of subdivision (g), the agency may comply with
21 this section by providing the security breach notification in
22 electronic or other form that directs the person whose personal
23 information has been breached to promptly change his or her
24 password and security question or answer, as applicable, or to take
25 other steps appropriate to protect the online account with the
26 agency and all other online accounts for which the person uses the
27 same user name or email address and password or security question
28 or answer.

29 (5) In the case of a breach of the security of the system involving
30 personal information defined in paragraph (2) of subdivision (g)
31 for login credentials of an email account furnished by the agency,
32 the agency shall not comply with this section by providing the
33 security breach notification to that email address, but may, instead,
34 comply with this section by providing notice by another method
35 described in this subdivision or by clear and conspicuous notice
36 delivered to the resident online when the resident is connected to
37 the online account from an Internet Protocol address or online
38 location from which the agency knows the resident customarily
39 accesses the account.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, “agency” includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

(l) *For purposes of this section, “encryption key” and “security credential” mean any information that could be used by an unauthorized person to access or decrypt encrypted personal information contained in a data system.*

SEC. 2. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized ~~person~~ *person, or, if the encryption key or security credential has, or is reasonably believed to have been, acquired by an unauthorized person at any time before or after the breach of security of the data, to a resident of California whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized* person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		

1		
2		
3		
4	What Information	
5	Was Involved?	
6		
7		
8		
9		
10	What We Are	
11	Doing.	
12		
13		
14		
15		
16	What You Can	
17	Do.	
18		
19		
20		
21	Other Important Information.	
22	[insert other important information]	
23		
24		
25		
26		
27		
28		
29		
30		Call [telephone number] or go to [Internet Web site]
31	For More	
32	Information.	
33		
34		

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain

1 language, shall be deemed to be in compliance with this
2 subdivision.

3 (2) The security breach notification described in paragraph (1)
4 shall include, at a minimum, the following information:

5 (A) The name and contact information of the reporting person
6 or business subject to this section.

7 (B) A list of the types of personal information that were or are
8 reasonably believed to have been the subject of a breach.

9 (C) If the information is possible to determine at the time the
10 notice is provided, then any of the following: (i) the date of the
11 breach, (ii) the estimated date of the breach, or (iii) the date range
12 within which the breach occurred. The notification shall also
13 include the date of the notice.

14 (D) Whether notification was delayed as a result of a law
15 enforcement investigation, if that information is possible to
16 determine at the time the notice is provided.

17 (E) A general description of the breach incident, if that
18 information is possible to determine at the time the notice is
19 provided.

20 (F) The toll-free telephone numbers and addresses of the major
21 credit reporting agencies if the breach exposed a social security
22 number or a driver's license or California identification card
23 number.

24 (G) If the person or business providing the notification was the
25 source of the breach, an offer to provide appropriate identity theft
26 prevention and mitigation services, if any, shall be provided at no
27 cost to the affected person for not less than 12 months along with
28 all information necessary to take advantage of the offer to any
29 person whose information was or may have been breached if the
30 breach exposed or may have exposed personal information defined
31 in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

32 (3) At the discretion of the person or business, the security
33 breach notification may also include any of the following:

34 (A) Information about what the person or business has done to
35 protect individuals whose information has been breached.

36 (B) Advice on steps that the person whose information has been
37 breached may take to protect himself or herself.

38 (e) A covered entity under the federal Health Insurance
39 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d
40 et seq.) will be deemed to have complied with the notice

1 requirements in subdivision (d) if it has complied completely with
2 Section 13402(f) of the federal Health Information Technology
3 for Economic and Clinical Health Act (Public Law 111-5).
4 However, nothing in this subdivision shall be construed to exempt
5 a covered entity from any other provision of this section.

6 (f) A person or business that is required to issue a security breach
7 notification pursuant to this section to more than 500 California
8 residents as a result of a single breach of the security system shall
9 electronically submit a single sample copy of that security breach
10 notification, excluding any personally identifiable information, to
11 the Attorney General. A single sample copy of a security breach
12 notification shall not be deemed to be within subdivision (f) of
13 Section 6254 of the Government Code.

14 (g) For purposes of this section, “breach of the security of the
15 system” means unauthorized acquisition of computerized data that
16 compromises the security, confidentiality, or integrity of personal
17 information maintained by the person or business. Good faith
18 acquisition of personal information by an employee or agent of
19 the person or business for the purposes of the person or business
20 is not a breach of the security of the system, provided that the
21 personal information is not used or subject to further unauthorized
22 disclosure.

23 (h) For purposes of this section, “personal information” means
24 either of the following:

25 (1) An individual’s first name or first initial and last name in
26 combination with any one or more of the following data elements,
27 when either the name or the data elements are not encrypted:

28 (A) Social security number.

29 (B) Driver’s license number or California identification card
30 number.

31 (C) Account number, credit or debit card number, in
32 combination with any required security code, access code, or
33 password that would permit access to an individual’s financial
34 account.

35 (D) Medical information.

36 (E) Health insurance information.

37 (F) Information or data collected through the use or operation
38 of an automated license plate recognition system, as defined in
39 Section 1798.90.5.

1 (2) A user name or email address, in combination with a
2 password or security question and answer that would permit access
3 to an online account.

4 (i) (1) For purposes of this section, “personal information” does
5 not include publicly available information that is lawfully made
6 available to the general public from federal, state, or local
7 government records.

8 (2) For purposes of this section, “medical information” means
9 any information regarding an individual’s medical history, mental
10 or physical condition, or medical treatment or diagnosis by a health
11 care professional.

12 (3) For purposes of this section, “health insurance information”
13 means an individual’s health insurance policy number or subscriber
14 identification number, any unique identifier used by a health insurer
15 to identify the individual, or any information in an individual’s
16 application and claims history, including any appeals records.

17 (4) For purposes of this section, “encrypted” means rendered
18 unusable, unreadable, or indecipherable to an unauthorized person
19 through a security technology or methodology generally accepted
20 in the field of information security.

21 (j) For purposes of this section, “notice” may be provided by
22 one of the following methods:

23 (1) Written notice.

24 (2) Electronic notice, if the notice provided is consistent with
25 the provisions regarding electronic records and signatures set forth
26 in Section 7001 of Title 15 of the United States Code.

27 (3) Substitute notice, if the person or business demonstrates that
28 the cost of providing notice would exceed two hundred fifty
29 thousand dollars (\$250,000), or that the affected class of subject
30 persons to be notified exceeds 500,000, or the person or business
31 does not have sufficient contact information. Substitute notice
32 shall consist of all of the following:

33 (A) Email notice when the person or business has an email
34 address for the subject persons.

35 (B) Conspicuous posting, for a minimum of 30 days, of the
36 notice on the Internet Web site page of the person or business, if
37 the person or business maintains one. For purposes of this
38 subparagraph, conspicuous posting on the person’s or business’s
39 Internet Web site means providing a link to the notice on the home
40 page or first significant page after entering the Internet Web site

1 that is in larger type than the surrounding text, or in contrasting
2 type, font, or color to the surrounding text of the same size, or set
3 off from the surrounding text of the same size by symbols or other
4 marks that call attention to the link.

5 (C) Notification to major statewide media.

6 (4) In the case of a breach of the security of the system involving
7 personal information defined in paragraph (2) of subdivision (h)
8 for an online account, and no other personal information defined
9 in paragraph (1) of subdivision (h), the person or business may
10 comply with this section by providing the security breach
11 notification in electronic or other form that directs the person whose
12 personal information has been breached promptly to change his
13 or her password and security question or answer, as applicable, or
14 to take other steps appropriate to protect the online account with
15 the person or business and all other online accounts for which the
16 person whose personal information has been breached uses the
17 same user name or email address and password or security question
18 or answer.

19 (5) In the case of a breach of the security of the system involving
20 personal information defined in paragraph (2) of subdivision (h)
21 for login credentials of an email account furnished by the person
22 or business, the person or business shall not comply with this
23 section by providing the security breach notification to that email
24 address, but may, instead, comply with this section by providing
25 notice by another method described in this subdivision or by clear
26 and conspicuous notice delivered to the resident online when the
27 resident is connected to the online account from an Internet
28 Protocol address or online location from which the person or
29 business knows the resident customarily accesses the account.

30 *(k) For purposes of this section, “encryption key” and “security*
31 *credential” mean any information that could be used by an*
32 *unauthorized person to access or decrypt encrypted personal*
33 *information contained in a data system.*

34 ~~(k)~~

35 (l) Notwithstanding subdivision (j), a person or business that
36 maintains its own notification procedures as part of an information
37 security policy for the treatment of personal information and is
38 otherwise consistent with the timing requirements of this part, shall
39 be deemed to be in compliance with the notification requirements
40 of this section if the person or business notifies subject persons in

- 1 accordance with its policies in the event of a breach of security of
- 2 the system.

O